Proxy Server Firewall shielding against traffic using known public VPS/Ns for IP disguising

Department of IT & Computer Sciences

Pak-Austria Fachhochschule Institute of Applied Sciences and Technology

Submitted To:

Dr. Abdul Waheed Khan
Engineer Hafsah Nasier

Submitted By:

Humza Asrar Ahmed

Dated: 16-01-2023

Introduction:

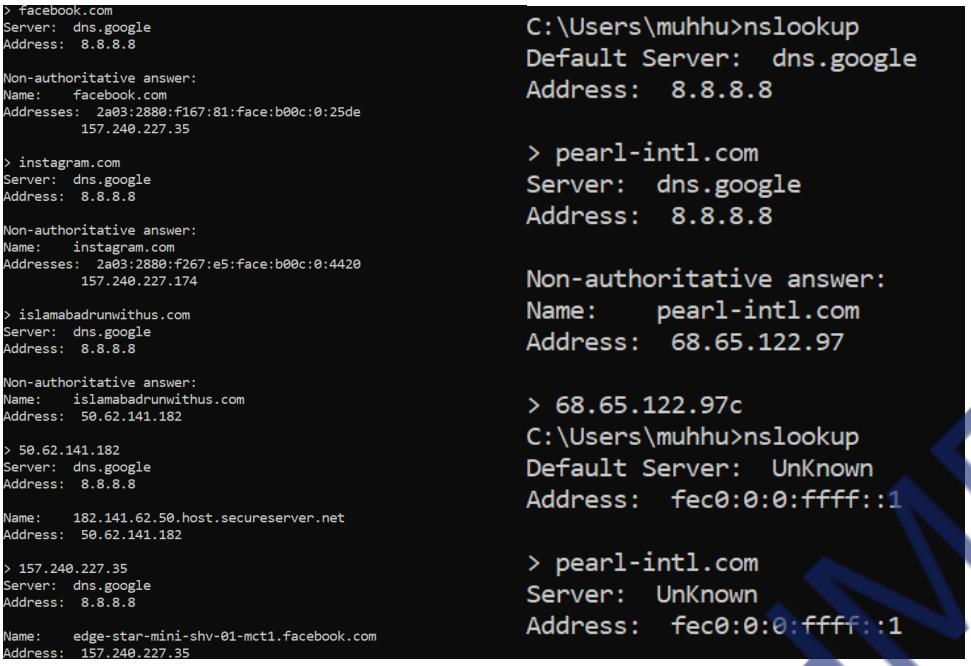
A proxy server that intercepts all the traffic passing through it and analyzes it's IP address. If it matches the known VPS/N provider IPs, then it will block the request and display a message of: 'Please turn off VPN service to browse or send files.' The firewall will be able to do this by matching the source IPs and packet headers with that of known VPNs IPs.

PfSense & Squid proxy server was used to deploy a proxy that was between the local client and the internet gateway router, thus logging and filtering all the data packets as per its configuration of it.

Aims & Objectives:

Deployed PfSense proxy server between the LAN clients and the internet gateway. The proxy had to be in the subnets of the routers IP to which the client is connecting to or else it won't be accessible(either internet, or proxy server would be accessible depending on the client's IP in subnet of the router or proxy server).

The proxy firewall rules set so that it blocks the traffic by IP depending upon choice. The DNS were still not blocked as they first resolve into IPs at the DNS server by it, and the DNS server then redirects the client to that requested website.



*Through **'nslookup'** in CMD.exe, the domain server request to its processing is displayed.*

Through using a tool ***'PfblockerNG'***, the domains were blocked through putting them in a list in '**DNSBL**' functionality of the mentioned tool, in '*DNSBL Groups*'. Hence when done, the config was reloaded and updated, then the firewall did as it said. I configured a list of Gambling and dating sited through calling a link that had all of them stored in it. The tool downloaded all the .txt data when updated and reloaded the config to block the updated links based on domain names.

Next was to understand the way a VPN works. A private IP requests the network router to connect/send data to the public VPN server IP. The request is carried out as by the router through its own public IP, and the connection is established through the router IP. Now the proxy either have to be between the router and the VPN server IP to block the connection between it, or the router must be configured not to talk to VPN servers' IP. As the proxy is between router and the client, I must find a method to make the proxy find out that the request and response of the client is from and for the VPNs' IP, and block it at the proxy even if the encrypted data has been arrived through the router. The best option is to block it when the client (private IP) initially requested the connection for VPNs IP, so that the request never reach the router and the router never fetches data from VPN servers.

I identified proton VPNs Japan IPs that it was assigning to me upon multiple connection establishments. Rather than identifying me as a client who is establishing connection and

breaking it again and again, it kept on servicing me and assigning their IP to me (a flaw). Hence when I identified majority of the IPs, I kept them in a list statically and put them in **DNSBL** functionality of ***'PfblockerNG',*** and blocked it, but haven't yet tested the working as their must me some Tunneling and stuff that I'm missing at the point.

In Squid proxy server, the IPs that were to be blocked reaching were mentioned in the configuration. It worked for blocking website access, though failed to stop VPN connection and data exchange due to tunnelling and stuff.

UFW firewall had also failed to do so(block VPN connection establishment) in a traditional manner.

Learning Outcomes:

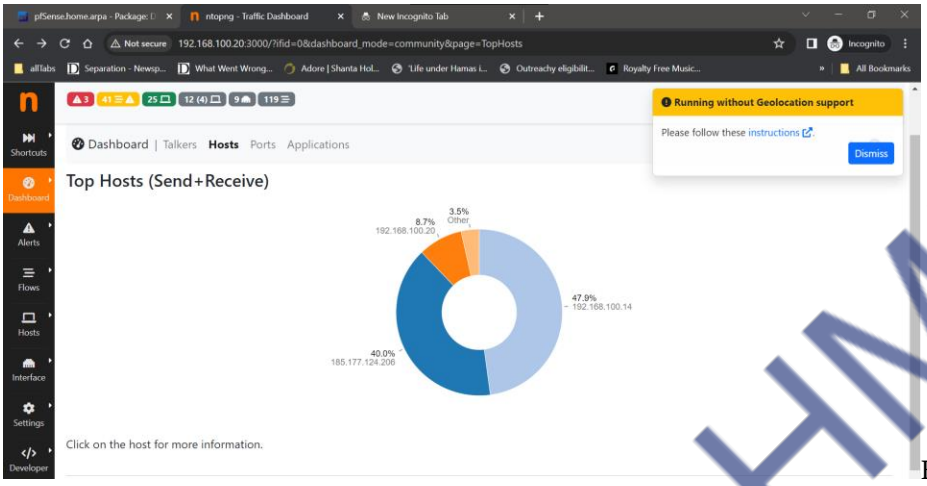
IPs divided in subnets can be accessed via subnet ranging. IP/32 subnet is 2^1, IP/24 subnet is 2^6 (256 addresses), etc. The subnets provide a range of IPs.

By default, the Squid proxy server was running in the localhost '127.0.0.1' which was though fine for the client itself upon which the proxy was running, but not for the LAN subnets that are required to go through the proxy. Hence through '**http_access 192.168.*.*:3128'**, a private IP was assigned to the proxy.

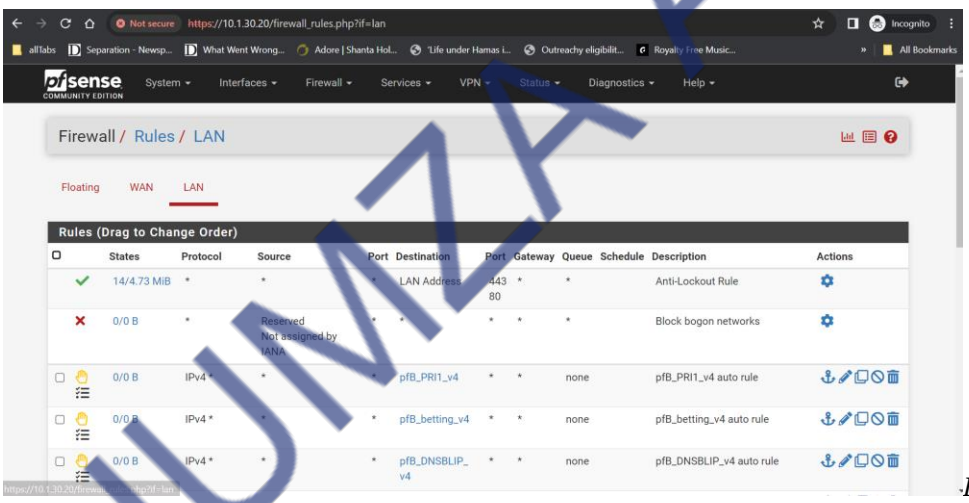
The configuration '**/etc/squid/squid.conf**' of Squid proxy server sequentialy executed the command i.e., it's interpreted language like bash in terminal and not compiled. The one at the bottom is exed later, hence what it says, even if negates the code above, is given priority and followed. It thus rewrites.

I noticed that when I do 'http_access deny all', it executed correctly and the firefox fails to fetch any results when browsed. Hence there isn't an issue with the requests not passing through the proxy serve. But when the IPs are blocked of VPNs, they don't comply as demanded in .conf file. I presume that websites will be blocked (without DNS, but IPs only), though I still have to test it.

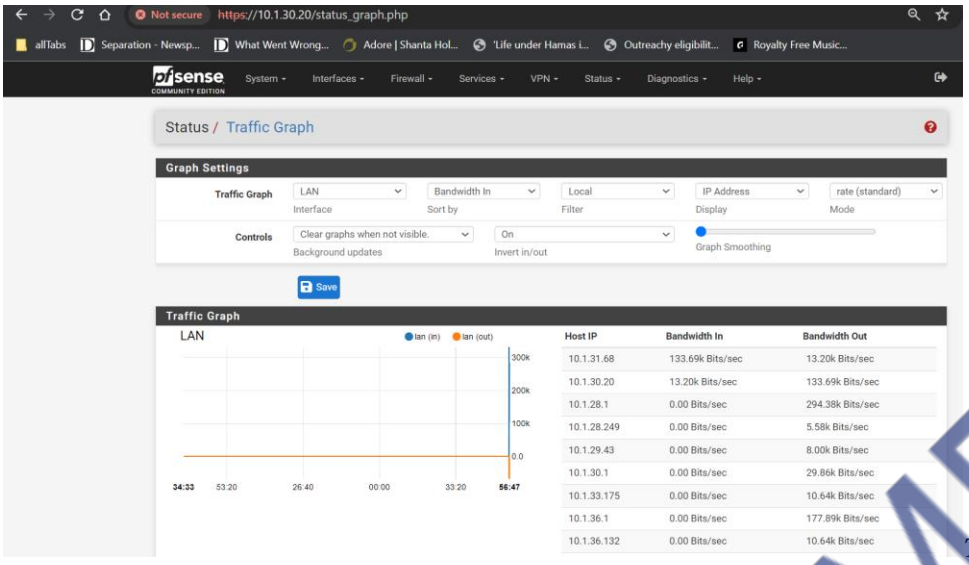
There are a lot of insites while checking, configuring and understanding the configuration of PfSense. I'll continue to use more features it provides. It really is a software glory.



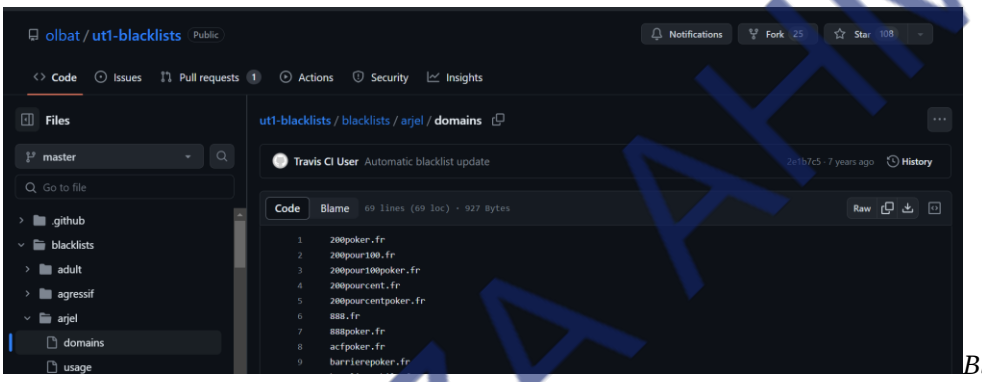
Hosts packets receive graph



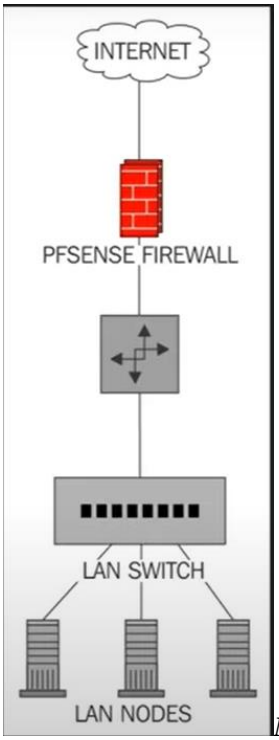
Firewall rules defining



Traffic graph



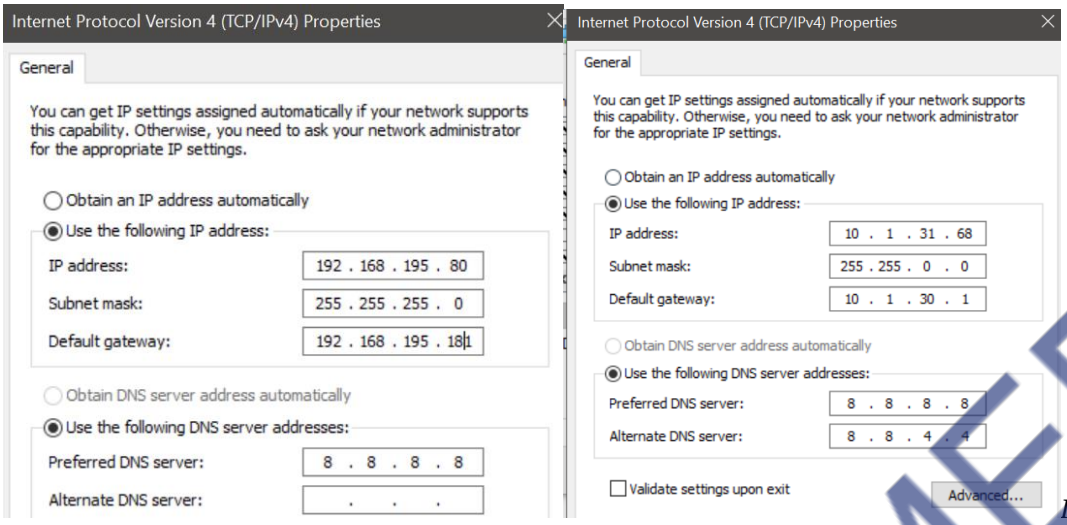
Blocklist URL



Mechanism of proxy server deployment

```
Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 10:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : home.arpa
   IPv4 Address. . . . . . . . . . . : 192.168.100.50
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.100.20

C:\Users\muhhu>
```

Ipconfig of IPv4 & router gateway



IPv4 inputting and manual definning in 'ncpa.cpl'

References

https://www.lifewire.com/how-to-find-your-default-gateway-ip-address-2626072

https://www.comparitech.com/blog/vpn-privacy/how-easy-is-it-to-detect-a-vpn-being-used/

https://www.comparitech.com/blog/vpn-privacy/what-is-browser-fingerprinting-how-to-protect-yourself/

https://www.youtube.com/watch?v=g2iSPBmRZ7M

https://www.youtube.com/watch?v=LEbAxsYRMcQ

https://www.youtube.com/watch?v=KWwOU1z5E8E

https://www.topbestalternatives.com/ccproxy/

https://www.technadu.com/what-port-does-vpn-use/281303/

https://www.digitalocean.com/community/tutorials/how-to-set-up-squid-proxy-on-ubuntu-20-04

https://wiki.squid-cache.org/RoadMap/

https://wiki.squid-cache.org/ConfigExamples/WebwasherChained

https://wiki.squid-cache.org/ConfigExamples/Intercept/LinuxLocalhost

https://wiki.squid-cache.org/ConfigExamples/Authenticate/WindowsActiveDirectory

https://www.makeuseof.com/best-networking-tools-replace-old-net-tools-linux/

https://www.scalahosting.com/kb/what-is-my-server-address/

https://www.ghacks.net/2010/06/19/restrict-network-access-by-time-or-ip-address-with-squid/

https://www.howtogeek.com/293213/how-to-configure-a-proxy-server-in-firefox/

https://serverfault.com/questions/305337/acl-allow-ip-range-squid

https://docs.netgate.com/pfsense/en/latest/monitoring/graphs/bandwidth-usage.html

https://superuser.com/questions/912610/difference-between-wan-ip-lan-ip

https://www.freshports.org/net/rsync

https://www.patreon.com/pfBlockerNG

https://www.comparitech.com/blog/vpn-privacy/setup-configure-pfsense/

https://docs.netgate.com/pfsense/en/latest/install/install-walkthrough.html

https://docs.netgate.com/pfsense/en/latest/packages/list.html

https://linuxincluded.com/using-pfblockerng-on-pfsense/

(configuration file of PfSense added in uploaded with this report)